VDSS IT SECURITY REQUIREMENTS
11/09/2004

State and Federal regulations require that sensitive data and personal information pertaining to VDSS systems be protected from unauthorized access. Only authorized personnel may access information.

System security requirements should include the following:

The system will use centralized security architecture. Responsibilities for security administration (add, remove users and modify access privileges) will be performed by the VDSS Information Security Unit.

Standard VDSS user logon IDs (consisting of the user's 3 initials and fips) should be used.

Applications making use of a database for the application back-end should not use application tables for user access into the system. If the application is web enabled, LDAP should be utilized for authentication and access control. This information should then be proxied (passed through) to user level accounts within the SQL database itself which will dictate access control.

Ie; WEB (Form login) -> LDAP -> Authenticated / Access Level YES -> Pass Form Info to SQL to get rights to tables.

If the system employs its own internal security the following must be provided:

- Passwords must comply with the Department's Password Policy as described in the Information Security Policy.
- Users must be prompted to change their password every 30 days.
- Passwords may be recycled and allowed by system every 12 months.
- Password must be encrypted at the server level.
- After 3 unsuccessful attempts to sign-on the password will be suspended.
- Central Office Security Officer's will reset passwords.
- All security-related activity (add, change, delete, password resets, failed logon attempts) must be recorded on an audit trail file along with the user's logon Id, security event, system date and time. This data must be available on a daily basis. Audit-reports from the audit trail files must be available to Central Office Information Security Unit. The audit trail file must be available on-line for 60 days for immediate retrieval, after which the information will be archived for 3 years.

The system must record all user access (inquiry and update) on an audit trail file to include the user's logon Id, record(s) accessed, system date and time. This data will be captured, and be available on a daily basis. A capability to generate audit-reports from the audit trail files will be available. The audit trail file will be available on-line for 60 days for immediate retrieval, after which the information will be archived for 3 years.

Automatic sign-off techniques must be in place when there is no activity within one hour. If there is no activity within 30 minutes, the system must prompt the user to re-enter the correct password. Three attempts are allowed. After the third attempt, if an incorrect password is entered, logon Id will be suspended. Central Office Information Security Unit can un-suspend locked accounts.

Only valid program functions and transactions will cause application programs to be executed. The users will not have direct access to data. User access to data will be controlled by authorized programs.

Users will only be able to update data within their specific region. Inquiry is permitted state-wide.

When a user's logon ID is deleted it may not be reused. The deleted logon Id data must remain on the system for audit trail and accountability purposes.

Security violation reports must be produced daily and forwarded to the Information Security Unit. These reports will show:

Three or more unsuccessful logon attempts
Users who have not logged in the past 60 days
Users attempting to run transactions they are not authorized to run.

Data will be encrypted.